MANUAL TRANSMITTAL

Department of the Treasury **Internal Revenue Service**

1.23.1

MAY 1, 2000

PURPOSE

This transmits new text for IRM 1.23 Section1, Personnel Security. It is a partial revision of the information contained in the former IRM 10.3.1.1, Internal Security Handbook.

NATURE OF MATERIALS

This Chapter discusses issues specifically relating to the functions and responsibilities of the IRS Personnel Security Office. There are other chapters that address personnel security and personnel security investigations. These are being issued under separate cover.

NATURE OF CHANGES

This IRM establishes the procedures for operation of the IRS Personnel Security Office in accordance with Treasury Order 102.17, Delegation Authority Concerning the Personnel Security Program, Treasury Directive 12-32, Delegation of Authority Concerning Personnel Security, dated October 17, 1997, and IRS Delegation Order 133, Authority to Perform Operating Functions Relating to Personnel Security, dated February 10, 1999.

EFFECT ON OTHER DOCUMENTS

This chapter supersedes IRM 10.3.1.1, Internal Security Handbook Chapter 11 Section 13.

Coby Stohrer
Personnel Security Officer

Table of Contents

In accordance with the Treasury Security Manual, TDP 71-10, Chapter I, Section 5, “Personnel Security Operations ”(09/21/98), the IRS Personnel Security Officer (PSO) will maintain personnel security operations in accordance with the procedures outlined therein.

1.23.1.1 (05-01-2000)
Personnel Security Files

(1) In accordance withTreasury Security Manual, Chapter I, Section 5, “Personnel Security Operations (09/21/98),” the Service will establish and maintain a personnel security file for each employee in the following positions:

- all national security positions
- all moderate and high risk public trust positions, and
- all those in low risk/nonsensitive positions on whom unfavorable or derogatory information has been developed or received.

(2) For purposes of personnel security, personal services contractors will be treated in the same manner as a Service employee. A file will also be established and maintained for each individual providing personal services who is covered by the provisions of Chapter II, Section 2 of the Treasury Security Manual.

(3) The Service will not maintain a file on a contract employee granted access to classified information under the National Industrial Security Program (NISP), unless there is a requirement for additional investigation in connection with access to:

- bureau facilities or automated information systems, or
- for access to classified information not covered under the NISP.

(4) With regard to favorable investigations on employees or contract employees in low or moderate risk positions, the Service will retain pertinent investigative information only.

(5) The Personnel Security Office maintains the personnel security files of employees (including employees of the Office of Chief Counsel) and contractors in two locations .

(6) All national security clearance files for holders of national security clearances that were active as of January 18, 1999, will be maintained in the Personnel Security Office. National security clearance files maintained on IRS employees who held a national security clearance prior to January 18, 1999, (i.e. the clearance was canceled and the file became ″inactive″ before that date) are maintained by the Treasury Inspector General for Tax Administration (TIGTA) Personnel Security Office. All requests to review the files maintained by the TIGTA, should be referred to that office.

(7) The Personnel Security Office will also maintain summary background investigation files for contractors on whom derogatory or adverse information was disclosed during the background investigation process and for whom an adjudication for access determination was made.

(8) Background investigation files of employees and contractors are maintained at the National Background Investigation Center (NBIC) in Florence, KY.

(9) Personnel security files will include documentation of investigative coverage and results, results of security and suitability adjudication/determinations, security clearance decisions, and any significant personnel security or suitability information which is developed during the employment.

(10) Personnel security files will be retained for the duration of the individual's employment or contractual relation with the Service and will be maintained in accordance with Treasury Directive (TD) 25-02, *Records Disposition Management Program and Removal of Records,* and National Archives and Records Administration General Records Schedule 18 (items 21-25 relating to personnel security files).

(11) Copies of the Office of Personnel Management (OPM) investigative reports will be retained for the duration of the retention schedule, however, the OPM case transmittal will be retained in the case file as the record of adjudicative action for a minimum of two years from the date of the final decision. Reports of Investigation of cases conducted by other Federal agencies but transmitted through OPM will be handled in the manner prescribed by the originating agency's Privacy Act system security notice or stamped caveats which may appear on those documents.

1.23.1.2 (05-01-2000)
Disposition of Investigative Reports

(1) Personnel security case files and related indices shall be destroyed or transferred to a Federal Records Center upon notification of an employee's death or not later than five years after the separation or transfer, or expiration of the contract relationship. Investigative reports and related documents obtained from other agencies for making security/suitability determinations shall be destroyed in accordance with the investigating agency's instruction.

1.23.1.3 (05-01-2000)
Certificate of Clearance and/or Security Determination

(1) For employees granted access to classified information, Treasury Department Form (TDF) 67-32.4 will be signed by the IRS Personnel Security Officer or other authorized official. The notification will document the date and basis of the determination, but shall not reflect any adverse information recorded in the personnel security file or on the Security Evaluation Sheet. When access to classified information has been granted, upgraded, administratively downgraded, suspended or cancelled, the form will be issued and will include the level of access granted, and, where appropriate, whether granted on an interim or final basis.

(2) For employees in public trust positions who do not require security clearances, IRS Form 2077 will be used to reflect at a minimum the completion date of the investigation, type of investigation, investigative agency, and type and date of suitability/security determination.

(3) The original copy of the Form TDF 67-32.4 or IRS Form 2077 will be filed on the right hand side of the Official Personnel Folder (OPF), while a copy shall be filed as the upper-most document in the personnel security file. The Personnel Security Office will be responsible for forwarding all forms TDF 67-32.4 to the OPF. NBIC will be responsible for forwarding all Forms 2077 to the OPF.

1.23.1.4 (05-01-2000)

National Security or Suitability Adjudication or Background Investigations Conducted on Employees of the PSO or NBIC

(1) To ensure independence of the adjudication and referral process and to eliminate any appearance of a conflict of interest in the handling of investigative reports conducted on employees of the Personnel Security Office and NBIC, the following procedures shall be effected:

a. All completed reports of investigations conducted for suitability or security purposes on employees of the Personnel Security Office or NBIC will be sent directly to the Personnel Security Officer and marked, “To be opened by addressee only.”
b. The Personnel Security Officer will be responsible for reviewing the completed background investigations for employees of the PSO or NBIC. After the review, the original copies of any favorably adjudicated reports of investigation conducted for national security clearance will be forwarded to the Chief, NBIC, for retention. A copy of the investigation will be maintained in the Personnel Security File.
c. For suitability investigations on employees of the PSO or NBIC who do not hold national security clearances, the Personnel Security Officer will review the report of investigation, and if favorable, forward the original copy to the attention of the Chief, NBIC, for retention. NBIC will be responsible for preparing the Form 2077 for the Official Personnel File. No copies will be maintained in the Personnel Security Office.
d. If after review of a report of investigation for suitability adjudication, the Personnel Security Officer determines that a referral to Labor Relations for a suitability determination/adjudication is appropriate, the report of investigation will be referred to the appropriate Labor Relations office with instructions to return the report of investigation to the Personnel Security Officer upon completion of their determination. The Personnel Security Officer will maintain a copy of the report of investigation until the original is returned . The Personnel Security Officer will then forward the original and all copies to the attention of the Chief, NBIC, for retention and completion of the Form 2077.

1.23.1.5 (05-01-2000)

Classified Information Nondisclosure Agreement (SF-312)

(1) As a condition of being granted access to classified information, the individual must first undergo a security briefing by appropriate security officers, of the PSO or other appropriate security officers acting on the authority of that office, wherein he or she is informed of the obligations and responsibilities attendant upon being granted such access, and must execute the SF-312, which shall be appropriately witnessed. For all IRS employees, the original SF-312 shall be placed on the right hand side of the OPF along with the copy of the TDF 67-32.4. A copy of the SF-312

may be retained in the employee's security file. For individuals not having an OPF, the SF-312 will be maintained in an appropriate system of records that meets applicable record disposition requirements. See General Records Schedule 18, item 25.

1.23.1.6 (05-01-2000)
Written Consent Form for Access to Financial Records

(1) Every employee granted access to classified information will provide the Service a written consent form developed by the Security Policy Board allowing an authorized investigative agency access to financial and other records as defined in Section 1.2(e) of Executive Order 12968, *Access to Classified Information,* during the duration of his or her access to classified information and for a period of three years thereafter. Such records may be requested by an authorized investigative agency only when:

a. there are reasonable grounds to believe, based on credible evidence, that the employee or former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;
b. a bureau has received credible information that an employee or former employee has incurred excessive indebtedness or has acquired a level of affluence that cannot be explained by other information; or
c. circumstances indicate that the employee or former employee had the capability and opportunity to disclose classified information that is known to have been lost or compromised to a foreign power or an agent of a foreign power.

Note: The Security Policy Board has yet to publish this consent form.

1.23.1.7 (05-01-2000)
Transfer of Personnel Security Records and Clearances

(1) In accordance with TDP 71-10, Chapter I, Section 5, when an employee transfers from one Treasury bureau to another, the complete personnel security file or a copy thereof shall be transferred from the personnel security office of the losing bureau to the personnel security office of the gaining bureau. However, where the file of an IRS employee contains tax information, the tax information shall not be transferred outside of the IRS.

(2) Pursuant to Section 2.4 of Executive Order 12968, a current security clearance is transferable between bureaus and agencies without readjudication of the investigation upon which it is based, provided:

a. a review of the current SF-86 discloses no adverse information and provided the existing investigation satisfies the investigative requirements for the new position in the Service, and
b. there is not otherwise known substantial information that the employee does not satisfy the general access eligibility standards of Executive Order 12968.

Further investigation will then be conducted only to meet required reinvestigation or security clearance revalidation requirements as outlined in Executive Order 12968.

1.23.1.8 (05-01-2000)

Protection of Personnel Security Records

(1) Information in personnel security investigations, records, and operations shall be carefully safeguarded to protect the interests of both the individual and the Service, pursuant to requirements of the Privacy Act. Unless classified at a higher level, personnel security information must be afforded the same degree of protection as material classified Confidential and must be used only for authorized official purposes. When not in use, personnel security information must be stored in a GSA-approved security container or in an equally secure area.

(2) Personnel security investigation information requested by subjects of investigations shall be processed according to procedures established by the Service under provisions of the Privacy Act or the Freedom of Information Act, as appropriate. Requests for the release of the results of any personnel investigation should be referred to the bureau or non-Treasury agency that conducted the investigation. When another agency requests a copy of an NBIC report of investigation under the routine use provision of the Privacy Act of 1974 (5 U.S.C. 552a), for the purpose of suitability or the granting of a security clearance, the request must be made in writing to the attention of the Disclosure Specialist within the IRS Personnel Security Office.

(3) When personnel security investigative information is disclosed to a third party (other than a Treasury Department employee working within the scope of his/her official duties), an accounting of the disclosure must be made in accordance with section 552a(c) of the Privacy Act [5 U.S.C. 552a(c)] and IRM 1.3.19, *Privacy Act Accounting for Disclosures.*, and a Form 5482, *Record of Disclosure* must be completed.

(4) Medical information developed during personnel security investigations may require interpretation by medical authorities in order to be meaningful to personnel security and operating officials, and its privileged nature shall be carefully respected.

(5) Investigative information and the identity of confidential sources must be safeguarded in accordance with the provisions of the Privacy Act.

(6) Reports containing classified information shall be protected in accordance with Executive Order 12958, *Classified National Security Information* (as amended), and appropriate Treasury regulations.

(7) When investigative information and/or personnel security files are made available for review by authorized personnel outside the IRS Personnel Security Office, for security or suitability purposes, a disclosure record, TDF 67-32.7, ″Security File Review,″ shall be prepared. The form must be signed and dated by those granted such access. In addition, the authorized personnel should provide a signed release form and must present credentials that identify them as authorized personnel. See paragraph 3 above regarding disclosure to third parties.

1.23.1.9 (05-01-2000)
Monitoring Personnel and Security Clearance Changes

(1) An effective personnel security program requires that personnel security officials be promptly informed of all personnel changes in order to assure that requisite investigations are obtained. Current data must be maintained on those who have been cleared to occupy sensitive positions or be granted access to classified information. Action should be taken to administratively withdraw or reduce the level of classified access as appropriate and to close out security files on separated employees.

(2) IRS Form 4323, *Notice of Status Change of Cleared Employee*, will be used by servicing personnel officers to notify the Personnel Security Office when an employee's status has changed. The Personnel Security Office will forward a copy of the form to NBIC for their records.

(3) The Personnel Security Office will send out periodic security clearance reviews to verify need-to-know access and security clearance level requirements for each cleared employee.

(4) Security Entry Tracking System (SETS) – In accordance with TDP 71-10, Chapter I, Section 5, the Service shall provide the Director, Office of Security, Department of Treasury, all security determinations and security clearances granted, revoked, suspended, or administratively withdrawn within the Service. This requirement applies to those occupying National Security sensitive positions.

(5) Similar personnel security information shall be provided on those in Moderate and High Risk public trust positions. The above information will be entered into the Department's tracking system, SETS. The availability of that information will facilitate granting access to classified information pursuant to Executive Order 12968.

(6) SETS also serves as an Office of Security locator file and provides preliminary security clearance information for special access programs.

(7) The Personnel Security Office will be responsible for data-entering all information for those employees who hold national security clearances. Servicing Personnel Offices will be responsible for data-entering all other investigative information for those employees in public trust positions in accordance with procedures outlined in IRM 1.23.2, *Security Investigations*, Chapter 3, *Background Investigations Processing Guide*.

1.23.1.10 (05-01-2000)
Clearance Verification

(1) Service employees assigned or on temporary duty outside the U.S. must comply with minimum security clearance and investigative requirements established by the Overseas Security Policy Board. (See Foreign Affairs Manual for applicable requirements.) Additional requirements for access to individual Embassies and other restricted facilities will be determined by the post.

(2) Service employees on TDY outside the U.S. must meet the security requirements established by the individual post(s) to be visited.

(3) Security clearances will be verified to posts as follows: The Service office preparing travel orders and notifying the post of the employee's arrival

should obtain the level of the employee's clearance from the IRS Personnel Security Office, and include this information in a cable to the post. (Example: "Mr. Jones holds a Top Secret clearance.") The security clearance information can be passed by telephone to the office preparing the cable, but the security office should be included for clearance on the cable, which will ensure that the security office is subsequently provided with a copy of the outgoing cable for inclusion in the individual's security file.

(4) Service employees visiting classified facilities, attending classified meetings, or requiring verification of clearance to another agency, should request clearance verification from the IRS Personnel Security Office via electronic mail, facsimile, or regular mail. The request must be made sufficiently in advance to allow for processing, and must include:

- Date of the visit or meeting
- Purpose
- Name and telephone of the contact person for the visit or meeting or to whom clearance information should be verified
- Name and fax number of the agency or office to which the certification needs to be sent

(5) The Personnel Security Office will prepare and fax a clearance verification memorandum to certify to the host or receiving agency security office the necessary security clearance status and other required data on the employee. Acceptance of temporary or interim security clearances is at the discretion of the agency whose facility is to be visited.

(6) When a Treasury employee of one bureau is detailed to another bureau, it is the responsibility of the bureau from which the employee is detailed to ensure that the employee meets all investigative requirements for the position into which the employee is detailed and to grant any security clearance required for access to classified information.

(7) For employees of other Federal agencies or cleared contractor facilities whose official duties require access to classified information at Service facilities, the sponsoring Service office shall request the IRS Personnel Security Office to obtain the pertinent security clearance verification data directly from the visitor's agency. For contractors, verification should be obtained from the parent company or the Defense Industrial Security Clearance Office.

1.23.1.11 (05-01-2000)

Suspension, Denial and Revocation of Access to Classified Information

(1) The Service will comply with the Treasury Security Manual, Chapter 1, Section 6, regarding suspensions, denials, and revocations of access to classified information, including its provisions on review proceedings for access eligibility determinations.

(2) The Personnel Security Officer will be the "Determining Official" for all such determinations within the Service.

(3) The Deputy Commissioner Operations will be the “Deciding Authority”for all such determinations within the Service.